

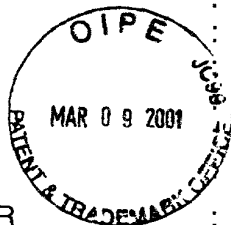
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Hatem TRABELSI

Serial No.: 09/740,800

Filed: December 21, 2000

For: DEVICE AND METHOD FOR
CONTROLLING ACCESS TO
RESOURCES

Examiner:

Group Art Unit:

Corres. To FR 99/16117
Filed December 21, 1999

McLean, Virginia

SUPPLEMENTAL PRELIMINARY AMENDMENTHonorable Commissioner of Patents and Trademarks
Washington, DC 20231

Sir:

Prior to examination of the above-identified application, please amend the application as follows:

IN THE SPECIFICATION:

Page 1, after the title and before the first paragraph, insert the following heading at the left-hand margin:

--Field of the Invention--;

Page 1, line 6, delete "The Prior Art" and substitute --Description of Related Art-- at the left-hand margin;

Page 2, line 15, delete "Presentation of the Figures" and substitute the following heading at the left-hand margin:

--Brief Description of the Drawings--;

Page 2, at line 27, delete "Description of an Embodiment of the Invention" and substitute the following heading at the left-hand margin:

--Detailed Description of the Preferred Embodiment(s)--;

Page 11, after the last paragraph ending "...lists.", insert the following new paragraph:

--While this invention has been described in conjunction with specific embodiments thereof, it is evident that many alternatives, modifications and variations will be apparent to those skilled in the art. Accordingly, the preferred embodiments of the invention as set forth herein, are intended to be illustrative, not limiting. Various changes may be made without departing from the true spirit and full scope of the invention as set forth herein and defined in the claims—

IN THE CLAIMS:

Please cancel claims 1 – 10 in their entirety and without prejudice and substitute the following new claims:

1 --11. A method for controlling access by a requestor (7) to resources (2d) in
 2 a distributed computer system (1) comprising defining conditions for obtaining a right
 3 to a resource (2d), assigning to the requester (7) at least one role based on an
 4 access control list, defining a part of a set of resources (2d) that is accessible by a
 5 given role by a validity domain, and utilizing the validity domain of the given role to
 6 restrict the resources accessible for the given role to only part of the resources.

1 12. A method according to claim 11, further comprising storing an
 2 additional piece of information relative to the need to consult the validity domain of
 3 the role in the access control list.

1 13. A method according to claim 12, further comprising consulting the
 2 additional information relative to the need to consult the validity domain of the role
 3 and verifying that the resource in question belongs to the validity domain only if
 4 required by said information.

1 14. A method according to claim 12, further comprising performing an
 2 access check on two levels:

- 3 ▪ a first-level check on the type of the resource (2d); and
- 4 ▪ a second-level check on the identifier of the resource (2d).

1 15. A method according to claim 14, wherein the first-level check verifies
 2 the existence of at least one entry of the access control list that satisfies conditions
 3 for obtaining a requested right of entry, and, if the right of entry exists, the existence
 4 of a validity domain for said entry.

1 16. A method according to claim 15, wherein the second-level check
 2 verifies, if a requested permission for right of entry contains a resource identifier, the
 3 existence of at least one configured permission corresponding to the requested
 4 permission and the value of the additional information relative to the need to consult
 5 the validity domain.

1 17. A method according to claim 11, further comprising grouping rights or
2 resources into generic groups represented by special characters or keywords or
3 other symbols.

1 18. A method according to claim 12, further comprising grouping rights or
2 resources into generic groups represented by special characters or keywords or
3 other symbols.

1 19. A method according to claim 13, further comprising grouping rights or
2 resources into generic groups represented by special characters or keywords or
3 other symbols.

1 20. A method according to claim 14, further comprising grouping rights or
2 resources into generic groups represented by special characters or keywords or
3 other symbols.

1 21. A method according to claim 15, further comprising grouping rights or
2 resources into generic groups represented by special characters or keywords or
3 other symbols.

1 22. A device for controlling access by a requestor (7) to interrogated
2 resources (2d) in a distributed computer system (1), comprising at least one
3 management machine (2a) (2b) (2c) (2d) organized into one or more networks (3),
4 said machine having at least one calling entity (4), for designating actions executed
5 by the requestor (7), an application program interface (5) for transmitting
6 interrogations from the calling entity, an access control service (6) for receiving said
7 interrogations and controlling access of the requestors (7) to the interrogated
8 resources (2d), storage means (10) (12) for storing roles, access control lists and
9 validity domains and means (9) (11) (13) for accessing the storage means.

1 23. A device for controlling access by a requestor (7) to interrogated
2 resources (2d) in a distributed computer system (1), according to claim 22, further
3 comprising means for defining conditions for obtaining a right to a resource, means
4 for assigning to the requestor at least one role based on an access control list, and

5 means for restricting the resources accessible for a given role to only part of the
6 resources by means of a validity domain of the role.

1 24. A device for controlling access by a requestor (7) to interrogated
2 resources (2d) in a computer system (1), according to claim 23, wherein the means
3 for storing stores an additional piece of information relative to the need to consult the
4 validity domain of the role in the access control list.

1 25. A device for controlling access by a requestor (7) to interrogated
2 resources (2d) in a computer system (1), according to claim 24, further comprising
3 means for consulting the additional information relative to the need to consult the
4 validity domain of the role and verifying that the resource in question belongs to the
5 validity domain only if required by said information.

1 26. A device for controlling access by a requestor (7) to interrogated
2 resources (2d) in a computer system (1), according to claim 25, further comprising
3 means for performing an access check on two levels:
4 ■ a first-level check on the type of the resource (2d); and
5 ■ a second-level check on the identifier of the resource (2d).

1 27. A device for controlling access by a requestor (7) to interrogated
2 resources (2d) in a computer system (1), according to claim 26, wherein a first-level
3 check verifies the existence of at least one entry of the access control list that
4 satisfies conditions for obtaining a requested right of entry to a resource, and, if the
5 entry exists, the existence of a validity domain for said entry.

1 28. A device for controlling access by a requestor (7) to interrogated
2 resources (2d) in a computer system (1), according to claim 27, wherein a second-
3 level check verifies if a requested right of entry to a resource contains a resource
4 identifier, the existence of at least one configured permission corresponding to the
5 requested right of entry and the value of additional information relative to the need to
6 consult the validity domain.

1 29. A software module for controlling access by a requestor (7) to
 2 resources (2d) of a computer system comprising means for defining conditions for
 3 obtaining a right of entry to a resource (2d), means for assigning to the requestor at
 4 least one role based on an access control list, means for defining a part of a set of
 5 resources (2d) that is accessible by a given role by a validity domain, and means for
 6 utilizing the validity domain of the given role to restrict the resources accessible for a
 7 given role to only part of the resources by means of a validity domain.

1 30. A software module for controlling access to resources according to
 2 claim 29, further comprising means for storing an additional piece of information
 3 relative to a need to consult the validity domain of the role in the access control list.

1 31. A software module for controlling access to resources according to
 2 claim 30, further comprising means for consulting the additional information relative
 3 to the need to consult the validity domain of the role and verifying that the resource
 4 in question belongs to the validity domain only if required by said information.

1 32. A software module for controlling access to resources according to
 2 claim 31, further comprising means for performing an access check on two levels:
 3 ▪ a first-level check on the type of the resource (2d); and
 4 ▪ a second-level check on the identifier of the resource (2d).

1 33. A software module for controlling access to resources according to
 2 claim 32 wherein the first-level check verifies the existence of at least one entry of
 3 the access control list that satisfies conditions for obtaining the requested right of
 4 entry, and, if the entry exists, the existence of a validity domain for said entry.

1 34. A software module for controlling access to resources according to
 2 claim 33 wherein the second-level check verifies, if the requested permission
 3 contains a resource identifier, the existence of at least one configured permission
 4 corresponding to the requested right of entry and the value of additional information
 5 relative to the need to consult the validity domain.--

TYSO01:9131914v0IT2147-906762I03\05\01

The present invention relates to a method, device and software module for controlling access by a requestor (7) to resources (2d) in a distributed computer system (1), consisting of defining roles that overlay one or more privileges and representing the requestor's authorization to perform specific tasks, of storing the defined roles in a memory or store (10, 12), and of storing an access control list that defines the conditions for obtaining a right to a resource type, i.e., a configured permission, in terms of privileges in said memory or store (10, 12) and utilizing a validity domain of a given role to restrict the resources accessible for a given role to only part of the resource.--

REMARKS

This Supplemental Preliminary Amendment is made to eliminate informalities in the specification, claims and abstract resulting from a literal translation of the French text, to eliminate the use of multiple dependent claims, and to insert headings to conform the application to U.S. practice.

The present application is believed to be in condition for examination, which action is earnestly solicited.

Respectfully submitted,

Miles & Stockbridge P.C.

Date March 9, 2001

By: 

Edward J. Kondracki
Registration No. 20,604

Miles & Stockbridge, P.C.
1751 Pinnacle Drive, Suite 500
McLean, Virginia 22102-3833
Tel.: (703) 903-9000